量子光計算処理(量子情報理論とその応用)

AUTHOR(S):

松枝, 秀明

CITATION:

松枝, 秀明. 量子光計算処理(量子情報理論とその応用). 数理解析研究所講究録 1994, 885: 29-45

ISSUE DATE:

1994-09

URL:

http://hdl.handle.net/2433/84296

数理解析研究所講究録
885巻 1994年 29-45

量子光計算処理

高知大学理学部情報科学科　松枝秀明（Hideaki Matsueda）

量子計算機ないしは量子情報処理は、その原理の実証結果の報告が、最近、見られるようになってきた。そのうち特に、光を用いた計算および処理につき、歴史的経過、主要な考察と提案、最近の研究結果等を論考する。

1 歴史的考察

量子情報処理の提案は、少なくとも1960年代後半にまで遡ることができる。当時、S.Wiesner によって、量子力学の不確定性原理に基礎をおく符号化の理論が提唱された［1］。偏光状態や½スピン等、不確定性原理に基づく共役な量を用いると、秘密通信や偽造防止貨幣が、理論上は可能になることが示されている。この提唱は、C.H.Bennett and G.Brassardによって採りあげられ、量子暗号理論として広められた。その実証も進められている［2］。波動関数や光子の自然放出を用いることも可能である［3］。

情報理論は、1948年の C.E.Shannon の論文［4］に始まるが、1970年代には整数論に基づく公開鍵暗号体系の構築等［5］、暗号理論の分野における結実が見られた。暗号の研究は、古代にまで遡ることができるが、第二次世界大戦のミッドウエー海戦等のとき、暗号解読力の差によって決定的な損失を被った事実は、いまだに日本人の記憶に残るところである。戦後に急成長した電子計算機およびそれを用いた情報システムの発達の根底に、

上述の情報理論が存在したことは論を待たない。

量子論を計算原理に適用する提唱もなされた。 1982年および1985年には、R.P.Feynman が量子計算機の原理と構造を示し、かつ、その実現可能性を推定した［６，７］。 量子力学のハミルトニアンを用いて、計算過程のエネルギー収支を表現し、超省エネルギー計算の可能性を論じた。 そこでは、計算時間と消費エネルギーとの間の不確定性による限界も考察された。後に、この量子計算機を実現させるための光素子の原理も提案された［８］。

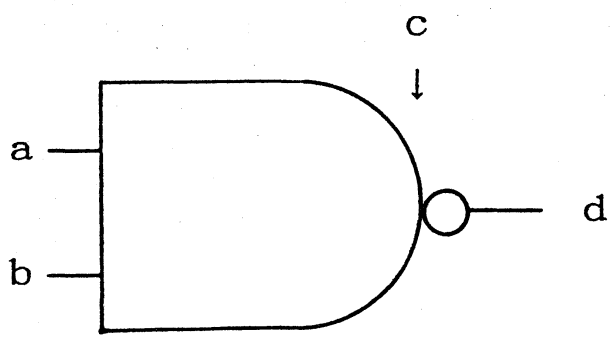
さらに、1985年および1989年に D.Deutch によって万能量子計算機が提唱された［９，１０］。 量子力学の時間依存ハミルトニアンを用い、連続変数である位相を含めて状態変化を表現する方法が採られた。

最近、磁束量子を用いた量子計算の原理が提唱され［１１］、かつ、実証も進められている。 また、多数個の電磁波ビームを用いる方法も提案されている［１２］。

２ Feynman の量子計算機に関する考究

２．１ 基本論理演算

現行の大型電子計算機のように複雑な計算をこなす電子回路も、ごく少数の基本回路ないしは基本素子の組み合わせによって実現する。 そこでは、一定電圧の有無が、論理値の１か０に対応している。 例えば、NOT(否定)とAND(論理積) とを組み合わせた機能を果たす基本素子、すなわちNAND（＝not and 、否定積）素子だけですべての論理演算を実行することができる。 このことは、ブール代数の基本公式を用いて証明される。 図１にNAND素子の構造と真理値表を示す。



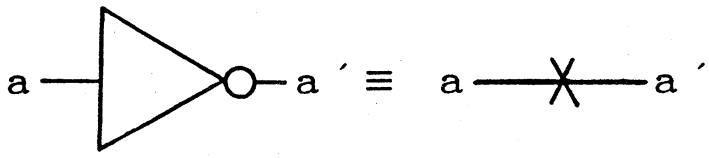
a	b	c	d
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	0

（a）　　（b）

図１　NAND素子の構造（ａ）と真理値表（ｂ）.

２．２　可逆基本論理素子

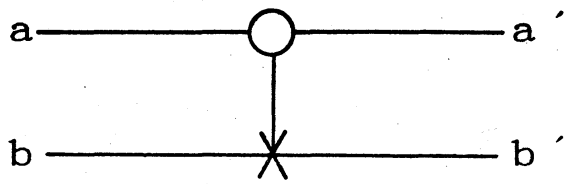
Feynman は、論理的に可逆変化をする素子（ゲート）のみによって構成され、計算機内部におけるエネルギー消費を限りなくゼロに近付け得る演算回路を、提案した［７］。　基本となる素子として、図２、図３、図４に示す３個すなわち NOT, CONTROLLED NOT, CONTROLLED CONTROLLED NOT が用いられた。　ここで、CONTROLLED NOTは図５に示すとうり、１個あるいは３個によって、それぞれFAN OUT あるいは EXCHANGE と呼ばれる機能（分配と交換）を果す素子となる。



a	a´
0	1
1	0

（a）　　（b）

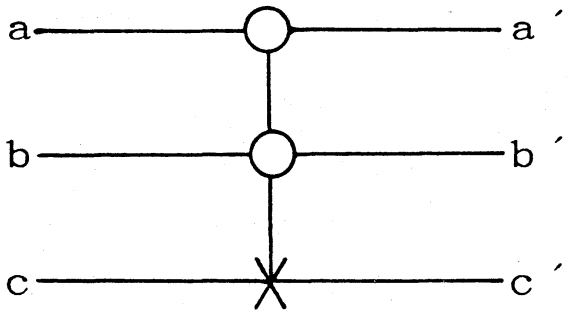
図２　NOT素子の構造（ａ）と真理値表（ｂ），［７］.



a	b	a´	b´
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

(a)　　(b)

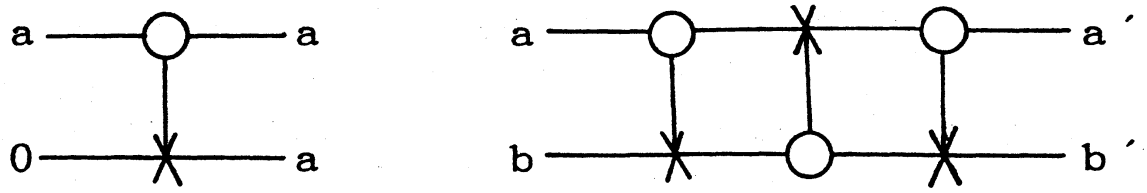
図３　CONTROLLED NOT　素子の構造（a）と真理値表（b），［7］.



a	b	c	a´	b´	c´
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

(a)　　(b)

図４　CONTROLLED CONTROLLED NOT 素子の構造（a）と真理値表（b），［7］.



（a） FAN OUT　　（b）EXCHANGE

図５　CONTROLLED NOT　素子の組合せ構造、 FAN OUT（a）および EXCHANGE（b），［7］.

さらに、CONTROLLED NOT素子３個とCONTROLLED CONTROLLED NOT 素子２個とにより、桁上り機能を含む全加算器が構成される。　一般に、全体の計算を遡行（逆行）するためには、計算途中の状況を記憶しておくことが必要となる。　出力する計算結果と同じだけの容量（ビット数）を余分に付加すれば、これが可能となり、可逆計算機になりうる。　このことは、入力、途中記憶、出力等に要する容量の時間経過に関する考察により明らかとなる。

２．３　量子可逆基本論理素子

次に、上述の可逆論理素子を、量子力学に従う２準位系によって構成する。　２準位系の発生原因としては、磁気スピンや偏光状態等を想定する。２準位間の状態遷移を、生成演算子ａ* および消滅演算子ａを用いて記述する。　これらは下記の行列に対応し、相互にユニタリー共役である。

$$a^* = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad a = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \qquad (1)$$

ａ* は、基底状態｜０〉$= \begin{pmatrix} 0 \\ 1 \end{pmatrix}$　に作用し、これを励起状態｜１〉$= \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ に変えるが、励起状態に作用した場合は、状態変化を起こさず、単に数０を生ずるものとする。　ａも同様に、励起状態｜１〉に作用し、これを基底状態｜０〉に変えるが、基底状態に作用した場合は、状態変化を

起こさず、単に数０を生ずるとする。　そして、状態を表示する数を
$N_a \equiv a^* a$　とすれば、励起状態に対し$N_a = 1$、基底状態に対し
$N_a = 0$　となる。　また、明らかに$1 - N_a = a a^*$ である。　なお、
関係式　$a a^* + a^* a = 1$　が成立し、単位行列に対応する。

さらに、前述の基本演算 NOTをA_a と表記すれば、

$$A_a = a + a^* \qquad (2)$$

となる。　CONTROLLED NOT　を$A_{a,b}$ と表記すれば、

$$A_{a,b} = a^* a (b + b^*) + a a^* \qquad (3)$$

となる。　CONTROLLED CONTROLLED NOT　を$A_{ab,c}$　と表記すれば、

$$A_{ab,c} = 1 + a^* a b^* b (c + c^* - 1) \qquad (4)$$

となる。　ここで、ａ，ｂ，ｃは図４に示す入出力線、ないしは演算が実行される場所を区別した消滅演算子であり、a^*，b^*，c^* は同意の生成演算子である。　今後用いるｄ，ｐ，ｑ，ｒ，ｓ，ｔ等も同様である。

２．４　量子可逆演算

以上の定義による演算はいずれもユニタリー行列によって表現され、その逐次的な組合せ、ないしは積による演算もユニタリー行列によって与えられる。　例えば、次の多次元行列Ｍは全加算器の一例を表現する。

$$M = A_{a,b} A_{b,c} A_{bc,d} A_{a,b} A_{ab,d} \qquad (5)$$

これは、右から順に$A_{ab,d}$、$A_{a,b}$ ・・・$A_{a,b}$ の演算が実行されることを表現する。　そして、その共役演算子M* は元(もと)の計算の遡行演算を意味する。

ここで、量子力学における時間発展が、初期状態の波動関数に指数因子 exp(iHt) を掛ける演算によって表現されることに着目する。　ただし、H はこの系のハミルトニアンである。　この指数因子 exp(iHt) を展開し、

$$\exp(iHt) = 1 + iHt - \frac{1}{2} H^2t^2 - \cdots \qquad (6)$$

とすれば、これを上述の基本演算（１）～（４）式の逐次的な作用、例えば（５）式のM等、に対応させることができる。　（６）式において H に関する高次の項は作用の繰返しを意味し、１回の繰返し毎に、基本演算が１段ずつ進むようにハミルトニアン H が組み立てられている。　その組み立て方法は次に示すとうりである。

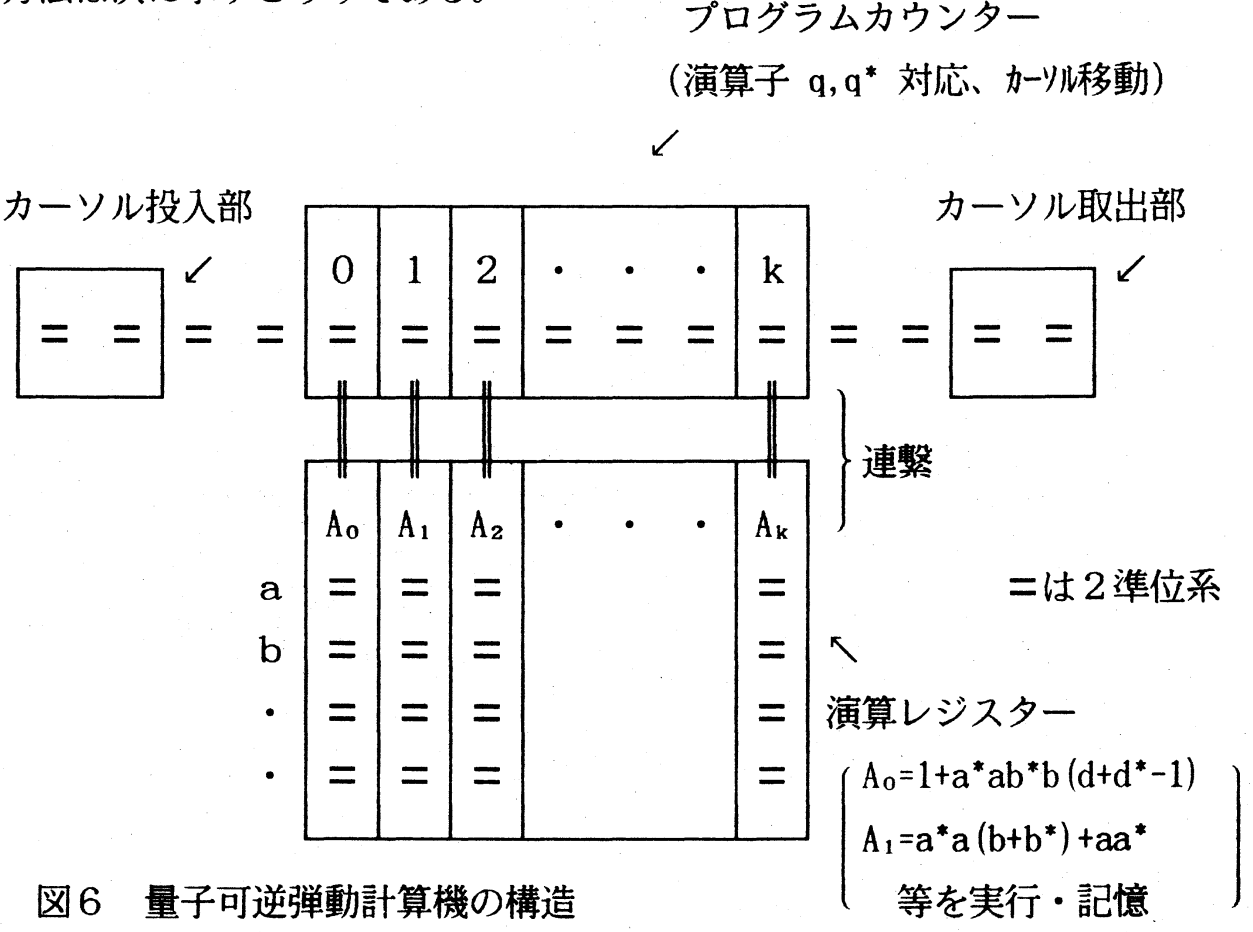


図６　量子可逆弾動計算機の構造

先ず、図６に示す構造の計算機を考える。　すなわち、所期の演算をする演算レジスターに、計算の進行を制御するプログラムカウンターを連繋し、かつ、そこへカーソル状態を投入する機構と、そこから取り出す機構とを付加する。　いずれにおいても、２．３節の２準位系が主な構成要素である。

次に、プログラムカウンターの２準位系にのみ作用する生成・消滅演算子をそれぞれ、q^*，q　によって表記する。　さらに、添字により位置も指定し、ｋ番目の２準位系にのみ作用する演算子をそれぞれ、q_k^*，q_k とする。　また、演算レジスターに作用する演算子は、（１）～（４）式と同様　a^*，a，b^*，b　等によって表記する。　そして、次のようにハミルトニアン Ｈ　を組立てる。

$$H = \sum_{i=0}^{k-1} q_{i+1}^* q_i A_{i+1} + c.c.$$

$$= q_1^* q_0 A_1 + q_2^* q_1 A_2 + q_3^* q_2 A_3 + \cdots$$
$$+ q_0^* q_1 A_1^* + q_1^* q_2 A_2^* + q_2^* q_3 A_3^* + \cdots \quad (7)$$

ここで、ｃ．ｃ．は共役項を意味し、A_i はｉ番目の演算を指し、その内容は（１）～（４）式等によって定義される。　共役項どうしは同一の演算の実行とその遡行（逆行）に対応する。

さて、図６の計算機において、カーソル投入部から、例えばスピン波の波束を投入すると、鎖状に配列した２準位系の（１次元格子の）上を、その波束は弾動的に、右端のカーソル取出部まで進む。その途上、プログラムカウンターに連繋された演算レジスターの中では、所期の演算が実行される。すなわち、（７）式のハミルトニアンの、一行目$q_1^* q_0 A_1 + q_2^* q_1 A_2 + \cdots$だけが丁度１回実行された直後の状態が実現する。これが求める計算結果である。

最初、演算レジスターに計算手順（アルゴリズム）、すなわちここでのハミルトニアンをプログラムする方法、および計算結果を読み取る方法等は今後の課題である。　また、プログラムカウンターと演算レジスターとの連繋の方法や、演算レジスターの内部構造等に関する研究は、現在進行中である［１３，１４］。

２．５　計算過程におけるエネルギー損失

図６に示した可逆弾動計算機において、プログラムカウンターの２準位系の鎖状配列（結晶）に格子欠陥が存在すると、カーソルである波束ないしは励起状態が、散乱される。　これは、弾動的な計算を阻害し、情報およびエネルギーの損失につながる。　ところが、完全な結晶を用いるか、あるいは、計算時間を十分長くすると、この散乱による情報エントロピーの損失、ないしは自由エネルギーの損失を任意に小さくすることができる。　そして、可逆計算機の所期の性能が発揮され、外部からのデーターの入力と、外部への計算結果の出力以外には、エネルギーを消費しない計算機が実現すると考えられる［７］。　ただし、ここでは、情報エントロピーがそのまま熱力学的なエントロピーに対応する場合を仮定している。　散乱に関する考察は次のとうりである。

励起状態が、前方に散乱され計算が本来の方向に１段階進む確率をP_fとし、後方に散乱され計算が１段階後退する確率をP_bとする。　両確率の和を総散乱確率と考え、Ｐと書けば、　$P = P_f + P_b$　となる。１回の散乱による、情報の獲得量は　$\ell n\, P_f^{-1}$　であり、情報の喪失量は$\ell n\, P_b^{-1}$　であると考える。　この場合、１回の散乱当たりの差引の損失量は、

$$\ell n \frac{1}{P_b} - \ell n \frac{1}{P_f} = \ell n \frac{P_f}{P_b}$$

$$\sim \frac{P_f - P_b}{P_f + P_b} = \frac{P_f - P_b}{P} \qquad (8)$$

となる。

ところで、カーソル等の励起状態が弾動的に移動する速度を v_r と書く。 これは、散乱によって前後ランダムに動く時の、瞬間速度である。散乱が全くない理想的な結晶では、この速度の弾動運動が実現すると考える。また、両散乱の結果、正味として所期の方向に移動する統計平均的な速度を v_d と書く。 これは、ドリフト速度と呼ばれる。 すると、

$$v_d = v_r \frac{P_f - P_b}{P_f + P_b} \qquad (9)$$

となる。 さらに、現実の計算時間を t_a とし、理想状態の最短計算時間を t_m とすれば、

$$\frac{t_m}{t_a} = \frac{v_d}{v_r} = \frac{P_f - P_b}{P_f + P_b} = \frac{P_f - P_b}{P} \qquad (10)$$

を得る。

演算1段階当りの情報損失量 ΔS は、(8)、(10)式を用い、

$$\begin{aligned} \Delta S &= P \times \{\text{散乱1回当たりの損失}\} \\ &= P \frac{P_f - P_b}{P_f + P_b} \\ &= P \frac{t_m}{t_a} \end{aligned} \qquad (11)$$

と計算される。 これが熱力学的なエントロピー損失と一致すると仮定すれば、対応する自由エネルギー損失 ΔF は次のように得られる。

$$\triangle F = kT\triangle S$$

$$= kTP\ \frac{t_m}{t_a}$$

$$= \frac{kT}{\frac{1}{P}\ \frac{t_a}{t_m}} \quad \rightarrow \quad 0 \quad (\ P \rightarrow 0 \quad or \quad t_a \rightarrow \infty \ ) \qquad (12)$$

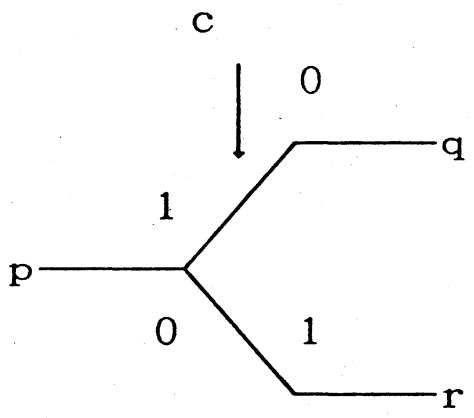
ここに、ｋはボルツマン定数であり、Ｔは演算素子の絶対温度である。　この式が前述の命題、「完全な結晶あるいは十分長い計算時間により、計算過程のエネルギー損失は任意に小さくなし得る。」を示すことは明白である。ここで、情報エントロピーがそのまま熱力学的なエントロピーに対応する場合を仮定していることは、先に述べたとうりである。

２．６　基本演算素子の単純化

以上の計算機は、図３、図４あるいは（３）式、（４）式によって定義された基本演算 CONTROLLED NOT と CONTROLLED CONTROLLED NOT を用いている。　ところが、これらを、さらに単純な分岐演算ないしはスイッチ演算に分解することができる。　この分岐演算の素子と機能を図７に示す。　対応するハミルトニアンは、

$$H = q^* cp + r^* c^* p + p^* c^* q + p^* cr \qquad (13)$$

である。　２個の分岐演算素子と１個の NOT素子とを、図８のように接続すれば、 CONTROLLED NOT 素子となる。　これらの図において、水平線はプログラムカウンターをあらわし、矢印は分岐方向を制御する機能を表現する。



if c = 1 go p to q and put c = 0

if c = 0 go p to r and put c = 1

if c = 1 go r to p and put c = 0

if c = 0 go q to p and put c = 1

図7　分岐演算素子［7］.

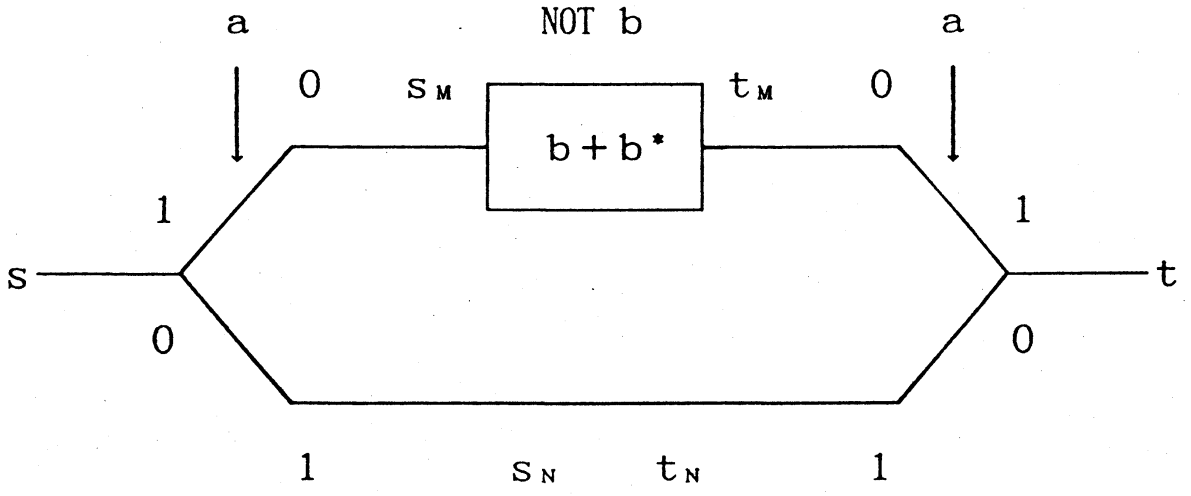


図8　分岐演算素子による CONTROLLED NOT 素子［7］.

図8の CONTROLLED NOT に対応するハミルトニアンは、

$$H = s_M^* a s + t^* a^* t_M + t_M^* (b+b^*) s_M + s_N^* a^* s + t^* a t_N + t_N^* s_N + c.c. \quad (14)$$

となる。

上記の分岐演算素子と NOT演算素子とを基本演算素子とすれば、万能的な機能を備えた量子可逆弾動計算機の設計と構築が、比較的容易になると考えられる。

3　Deutchの万能量子計算機に関する考究

前節に述べた Feynmanの発表［6，7］等を受け、1985年および1989年に D.Deutsch　は、万能量子計算機の可能性につき、計算可能性の理論と量子力学とに基づいて論考した［9，10］。　Church-Turing の提唱と、計算結果等の測定に関する量子力学的および熱力学的な限界との、対応関係の検討等から、量子計算機の現実的な意味づけが考察された。　さらに、基本演算素子の構造と、行列によるその表現が提案された。

計算過程を、量子力学のシュレーディンガー方程式に基づく時間発展に対応させる。　そこでは、波動関数が計算機の状態を表現する。　しかも、前述の Feynmanの構想をさらに進め、時間に顕に依存するハミルトニアンを考える。　そして、論理変数の数に応じ、1個の万能な基本演算素子を考案する。　これと、論理値1（励起状態）および論理値0（基底状態）のそれぞれを発生させる素子と、単なる接続（単位元）とだけを用いて、万能量子計算機を組み立てる。

NOT演算に関しては、その万能化された演算機能として、NOT の累乗と累乗根の演算が次のように定義される。　先ず NOT演算を行列S_Nと書けば、（1）、（2）式同様、

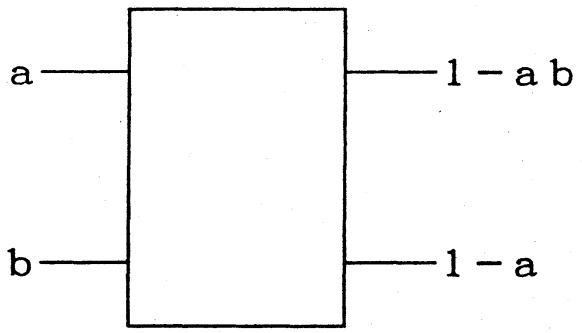
$$S_N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (15)$$

となる。　次に実数パラメーター（位相）αに対し、S_N のα乗を、

$$S_N^{\alpha} = \frac{1}{2}\begin{pmatrix} 1 + \exp(i\pi\alpha) & 1 - \exp(i\pi\alpha) \\ 1 - \exp(i\pi\alpha) & 1 + \exp(i\pi\alpha) \end{pmatrix} \quad (16)$$

とする。　これは NOT演算をα回繰り返す操作であるが、αが非整数の場合は、 NOT演算の累乗根演算を定義する。　この演算は従来の古典的な計算機に類を見ない。　なお、αが奇数の場合、S_N のα乗は単なるS_N すなわち NOT 演算に帰着し、αが偶数の場合は単位行列ないしは単位元となる。

２変数（２ビット）演算の場合、図９に示す構造が万能な基本演算素子であり、NAND/NOT演算素子（ゲート）と呼ばれる。



（a）

a	b	1-ab	1-a
0	0	1	1
0	1	1	1
1	0	1	0
1	1	0	0

（b）

図９　NAND/NOT素子の構造（ａ）と真理値表（ｂ），［１０］.

さらに、３，４変数および任意のｎ変数の場合について、万能な基本演算素子を組み立てることができる。　そこでは、 NOT演算の累乗根素子が使われる。

従来の論理演算素子の場合は、素子相互の機能の異同が数量的に明確であり、その集合は離散的に分布する。　ところが、Deutsch の万能量子計算機の素子の場合は、そこに含まれる NOT演算の累乗根が連続パラメーターαを伴うので、その集合は連続的に分布する。　この点では、物理量を離散的な固有値を用いて表現する量子力学や、アナログ画像信号を時間、空間、強度に関して離散的なデジタルパルスに変換する量子化処理等における、通例の量子化がなされた系とは事情を異にする。

この万能量子計算機の素子は、パラメーターαに関し、連続的に変化する状態を取り得る。　しかし、現実の計算においては、測定や認識の精度の限界に応じて、ある有限の微小な幅を設定し、その範囲内に入る状態をまとめて１状態とみなす方法が妥当と考えられる。　パラメーターαに着目し、この計算機の実現性に関する考察を進めることが可能である。　また、現実にαとして用いる物理量に関する研究が進行中である［１３，１４］。

４　結　　言

量子情報処理の歴史を考察し、量子暗号理論、量子計算機の提案、最近の研究動向等を概観した。　特に Feynmanの量子計算機につき、そこに用いられる可逆基本論理素子、分岐演算素子、量子可逆弾動計算機の構造、エネルギー損失、将来の可能性等を詳しく論じた。　また、Deutchの万能量子計算機につき、基本論理素子、 NOT演算の累乗根演算、将来の可能性等を論じた。

将来は、物理的な実体を基礎に踏まえ、実証を含めた研究が進められることが望ましい。　中でも、偏光、電磁波ビーム、磁束量子等に関する理論と実験が有望と考える。　この方向の研究を継続させて行く考えである。

5 文　献

[1] Stephen Wiesner, "Conjugate Coding", SIGACT News 15, 78-88 (1983).

[2] Charles H. Bennett and Gilles Brassard, "The dawn of a new era for quantum cryptography: The experimental prototype is working!", SIGACT News 20, 78-82 (1989).

[3] Hideaki Matsueda, "Methods of Quantum Cryptograph", The 1994 Symp. Cryptography and Information Security, Biwako, Japan, paper SCIS94-15A, Jan. 29 (1994).

[4] C. E. Shannon, "A Mathematical Theory of Communication", part I-II, III-V, Bell Syst. Tech. J. 27, 379, 623 (1948).

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications ACM 21, 120-126 (1978).

[6] Richard P. Feynman, "Simulating Physics with Computers", Int. J. Theor. Phys. 21, 467-488 (1982).

[7] Richard P. Feynman, "Quantum Mechanical Computers", Optics News 11, 11-20 (1985).

[8] G. J. Milburn, "Quantum Optical Fredkin Gate," Phys. Rev. Lett. 62, 2124-2127 (1989).

[9] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer", Proc. R. Soc. Lond. A 400, 97-117 (1985).

[10] D. Deutsch, "Quantum computational networks", Proc. R. Soc. Lond. A 425, 73-90 (1989).

[11] E. Goto, N. Yoshida, K. F. Loe, and Willy Hioe, "A Study on Irreversible Loss of Information without Heat Generation", Proc. 3rd. Int. Symp. Foundations of Quantum Mechanics, Tokyo, 412-418 (1989).

[12] A. Zeilinger, "Controlling Entanglement in Quantum Optics", Abs. Int. Workshop on Quantum Control and Measurement, (a satellite of 4th. Int. Symp. Foundations of Quantum Mechanics; ISQM-SAT), Hatoyama, PL2, 2 (1992).

[13] 松 枝 秀 明 「光・電子集積回路の物理」 裳華房, 応用物理学選書 7 (1989).

[14] Hideaki Matsueda, "Physical Basis of Optoelectronic Integration", Chap. 2 of 'Optoelectronic Integration', O. Wada ed., Kluwer Academic, Boston, pp.17-60, 1994.